Attorney Matter No. 290.1078APP

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS AND INTERFERENCES

In re application of: Sami Vaarala et al

Serial No. 10/500,930

Filed: 19 October 2005

For: METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

APPEAL BRIEF

Art Unit 2458

Examiner Afshawn M. Towfighi

Date: 22 June, 2010

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANT'S BRIEF ON APPEAL

Real Party in Interest

The real party in interest is MPH Technologies Oy, Tekniikantie 14, FIN-02150 Espoo, Finland, the recorded assignee of the above-captioned patent application.

Related Appeals and Interferences

No related appeals or interferences of this application are known to the Appellant, the Appellant's legal representative or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status of the Claims

Rejection 1

Claims 1-5, 7-10, 22-24 and 26-27 stand rejected in the Office action dated 23 March 2010 as being anticipated by US Patent Application No. 2001/0047487 to Linnakangas et al.

Rejection 2

Claims 6, 11-14, 20-21 stand rejected in the Office action dated 23 March 2010 as being obvious over Linnakangas in view of Applicant's Admitted Prior Art (AAPA).

Rejection 3

Claims 15-19 and 25 stand rejected in the Office action dated 23 March 2010 as being obvious over Linnakangas in view of Sandhu.

The application has been rejected at least twice. A copy of the claims is reproduced as Claims Appendix hereto. The rejections of claims 1-27 are appealed.

Status of Amendments

All Amendments have been entered.

Summary of Claimed Subject Matter

The application has three independent claims (i.e. claims 1, 22 and 27). Independent claim 1 refers to a method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network (see abstract and paragraph 0039 of US 2006/0173968). The first computer and the second computer negotiate and exchange keys according to a key exchange protocol to establish a secure connection (such as a security association (SA)) between the first computer and the second computer via the intermediate computer (see paragraphs 0039, 0070, 0104-0113). The secure connection has a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection (see Figs. 1-2, paragraphs 0010, 0013-0014 and 0021). A secure message is formed in the first computer by giving the secure message a first unique identity and a first destination address to the intermediate computer (see abstract, paragraphs 0039, 0041, 0043-0044). The secure message is sent from the first computer to the

intermediate computer (see abstract). The intermediate computer receives the secure message and performs a translation by using the first unique identity to find a second destination address of the second computer (see paragraphs 0023, 0041, 0045-0048, 0053-0060, 0072-0095). The intermediate computer substitutes the first destination address with the second destination address to the second computer (see abstract, original claim 1, paragraphs 0039 and 0086). The intermediate computer substitutes the first unique identity with a second unique identity of the same secure connection without establishing a new secure connection between the intermediate computer and the second computer and without involving the second computer (see abstract, paragraphs 0039, 0047 and 0086). The intermediate computer then forwards the secure message with the second destination address and the second unique identity to the second computer in the same secure connection (see abstract, Figs. 1-2, paragraphs 0039, 0041, 0045-0048, 0052-0061, 0070-0076, 0083-0090, 0096-0118).

Claim 2 refers to the step of forming the secure message by using an IPSec connection between the first computer and the second computer (see original claim 2, paragraphs 0009, 0024-0033, 0043 and 0045).

Claim 3 refers to the step of performing a secure forwarding of the message by making use of SSL or TLS protocols (see original claim 3).

Claim 4 refers to the step of manually performing a preceding distribution of keys to components for forming the IPSec connection (see original claim 4).

Claim 5 refers to the step of performing a preceding distribution of keys for forming the IPSec connection by an automated key exchange protocol (see original claim 5).

Claim 6 refers to the step of performing the automated key exchange protocol used for the preceding distribution of keys for forming the IPSec connection by means of a modified IKE key exchange protocol between the first computer and the intermediate computer and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer (see original claim 6 and paragraphs 0018, 0024 and 0043-0062).

Claim 7 refers to the step of sending the message that is sent from the first computer as a packet that contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer, the unique identity (see original claim 7, paragraphs 0041-0062, 0082-0091).

Claim 8 refers to the IPSec connection being one or more security associations (SA) and the unique identity being one or more SPI values (see original claim 8).

Claim 9 refers to the step of performing the matching by using a translation table stored at the intermediate computer

(see original claim 9 and paragraphs 0041-0048, 0086, 0090, 0149-0150 and 0214-0216).

Claim 10 refers to the step of changing both the address and the SPI-value by the intermediate computer (see original claim 10 and paragraphs 0043-0046).

Claim 11 refers to the first computer being a mobile terminal so that the mobility is enabled by modifying the translation table at the intermediate computer (see original claim 11 and paragraphs 0020-0033, 0079-0085).

Claim 12 refers to the step of performing the modification of the translation tables by sending a request for registration of the new address from the first computer to the intermediate computer (see original claim 12).

Claim 13 refers to the step of sending a reply to the request for registration from the intermediate computer to the first computer (see original claim 13).

Claim 14 refers to the step of authenticating or encrypting by IPSec the request for registration and/or reply (see original claim 14 and paragraphs 0051, 0073 and 0081).

Claim 15 refers to the step of establishing the key distribution for the secure connections by establishing an IKE protocol translation table, and using the translation table to modify IP addresses and cookie values of IKE packets in the intermediate computer (see original claim 15 and paragraphs 0039-

0062 and 0111-0142).

Claim 16 refers to the step of establishing the key exchange distribution by generating an initiator cookie and sending a zero responder cookie to the second computer, generating a responder cookie in the second computer, establishing a mapping between IP addresses and IKE cookie values in the intermediate computer, and using the translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets (see original claim 16 and paragraphs 0039-0062).

Claim 17 refers to the step of modifying a modified IKE protocol between the first computer and the intermediate computer by transmitting the IKE keys from the first computer to the intermediate computer in order to decrypt and modify IKE packets (see original claim 17 and paragraphs 0039-0062).

Claim 18 refers to the step of carrying out in a modified IKE protocol between the first computer and the intermediate computer the modification of the IKE packets by the first computer with the intermediate computer requesting such modifications (see original claim 18 and paragraphs 0039-0062).

Claim 19 refers to the step of defining the address so that the first computer is identified for the second computer by the intermediate computer by means of an IP address taken from a pool of user IP addresses when forming the translation table (see

original claim 19).

Claim 20 refers to the step of sending the secure message by using an IPSec transport mode (see original claim 20).

Claim 21 refers to the step of sending the secure message by using an IPSec tunnel mode (see original claim 21).

Independent claim 22 refers to a telecommunication network for secure forwarding of messages that has a first computer, a second computer and an intermediate computer (see abstract and paragraph 0039). The network has means for negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a security association (SA) that has a source address of the first computer as a first end point and a destination address of the second computer as a second end point (see Figs. 1-2, paragraphs 0010, 0013-0014, 0021, 0039-0062, 0070 and 0104-0113). The first and the second computers have means for performing IPSec processing (see paragraphs 0009, 0024-0033, 0043-0045 and 0054). The intermediate computer has translation means for using translation tables to perform IPSec and IKE translation and for changing a destination address of the intermediate computer of a secure message to a destination address of the second computer (see paragraphs 0020-0033, 0043-0062 and 0079-0085). Furthermore, the intermediate computer has means for forwarding the secure message received from the first

computer to the second computer in the same security association (see paragraph 0039).

Claim 23 refers to the translation table for IPSec translation has IP addresses of the intermediate computer to be matched with IP addresses of the second computer (see original claim 23 and paragraphs 0046-0062).

Claim 24 refers to the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate computer and the second computer (see original claim 24 and paragraphs 0046-0062).

Claim 25 refers to both partitions of the mapping table for IKE translation contains translation fields for a source IP address, a destination IP address, initiator and responder cookies between respective computers (see original claim 25 and paragraphs 0049, 0054 and 0058).

Claim 26 refers to another translation table for IKE translation containing fields for matching a given user to a given computer (see original claim 26 and paragraphs 0041-0048, 0086, 0090, 0149-0150 and 0214-0216).

Independent claim 27 refers to a telecommunication network for secure forwarding of messages that has a first computer, a second computer and an intermediate computer

electronically connected to the first computer and the second computer (see abstract and paragraphs 0039. The network has means for negotiating and exchanging keys between the first computer and the second computer to establish a secure connection therebetween that has a source address of the first computer as a first end point and a destination address of the second computer as a second end point (see paragraphs 0039, 0041-0062, 0070 and 0104-0113). The intermediate computer has means for performing translation between destination addresses and secure identities for forwarding secure messages received from the first computer to the second computer in the same secure connection (see paragraphs 0023, 0041, 0045-0048, 0053-0060 and 0072-0095).

In summary, one problem with standard/conventional IPSsec mobile telephone systems is that the end points of the IPSec tunnel mode SA (security association) are fixed. There is no feature in conventional systems for changing any of the parameters of an SA other than by establishing a new SA that replaces the previous SA. More particularly, since mobile terminals move and thus change their network points frequently and since IPSec connections are bound to fixed addresses, the mobile terminals must establish new IPSec connections from each new point of attachment. This requires the exchange of keys etc. which is a cumbersome process that uses computation time. The method of the present invention provides a solution to this

problem.

Unique features of the present invention are the secure connection is established all the way between the first computer and the second computer via the intermediate computer by exchanging keys and that the intermediate computer 1) uses the first unique identity to find a second destination address to the second computer and 2) substitutes the first destination address with the second destination address in the same secure connection. Thus, there is no need to set up a new secure connection between the intermediate computer and the second computer. In this way, a secure message, sent from the first computer to the intermediate computer, may be modified by the intermediate computer so that it can be forwarded from the intermediate computer to the second computer in the same secure connection without requiring the cumbersome exchange of additional keys to set up a new secure connection between the intermediate computer and the second computer and without involving the second computer.

Grounds Of Rejection To Be Reviewed On Appeal

Whether the Examiner properly rejected claims 1-5, 7-10, 22-24 and 26-27 as being anticipated by Linnakangas and whether the Examiner properly rejected claims 6, 11-14 and 20-21

of the application as being obvious of Linnakangas in view of Applicants' Admitted Prior Art (AAPA). Finally, whether the Examiner properly rejected claims 15-19 and 25 of the application as being obvious of Linnakangas in view of Sandhu.

Argument (Rejection 1) - 35 U.S.C. 102 (Anticipation)

The 102 rejection is submitted to be improper because the cited Linnakangas reference (US 2001/0047487) does not, among other things, teach or suggest the steps establishing a secure connection between the first and second computer that requires the first and second computer to exchange keys between each other when establishing the secure connection so that the secure connection has a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection. Additionally, Linnakangas fails to teach the step of the intermediate computer substituting the first destination address and first unique identity of the secure message with a second destination address and a second unique identity of a second computer in the same secure connection without establishing a new secure connection and without involving the second computer so that the intermediate computer forwards the secure message to the second computer in the same secure connection. Linnakangas merely teaches the step of setting up of a secure connection (security association) between the intermediate computer (router 2) and the second computer (remote hosts 4) and the prior segment between the intermediate computer and the first computer (local hosts 5) is merely within the same local area network (LAN) so that the intermediate computer decrypts packets going into the local hosts

5 of the LAN and encrypts packets going out from the local hosts 5 of the LAN to the second computer. If the segment between the intermediate computer (router 2) and the first computer (local hosts 5) had been part of the same security association there would be no need to decrypt and encrypt messages going to and from the first computer (local hosts 5). The decryption/encryption procedure of Linnakangas' intermediate computer (router 2) is quite different from sending a secure message in a secure connection that extends all the way from the first computer (local hosts 5) to the second computer (remote hosts 4). The above features are submitted to be novel and not obvious in view of the cited references.

More particularly, Linnakangas describes the establishment of a security association (which is one type of a secure connection). When a security association is formed between two computers, keys are first exchanged between the two computers. This is done according to an Internet Key Exchange (IKE) protocol and the security association is defined by unique identity and addresses of the two computers between which the security association is formed. Despite numerous efforts to try to explain in Linnakangas there is no security association established between the local hosts 5 (first computer) and the router 2 (intermediate computer), the Examiner still maintains that there is also a security association created between the

router 2 and the local hosts 5. Appellants maintain that there is only a security association created between the router 2 (intermediate computer) and the remote hosts 4 (second computer). It is submitted that the security association established does not extend to the local hosts 5 (first computer).

The Examiner refers to paragraphs 4 and 5 of Linnakangas as teaching the establishment of the secure connection between the first computer and the second computer.

Appellants respectfully disagree. Paragraphs 4 and 5 describe the establishment of security associations (SAs) in general and not that a SA is established between the remote hosts 4 and local hosts 5 or between the intermediate computer 2 and the local hosts 5. It is submitted that paragraph 24 of Linnakangas clearly teaches that each remote host 4 must negotiate at least one pair of SAs with the router 2. Linnakangas fails to teach the remote hosts 4 negotiating and establishing a security association with the local hosts 5. More importantly, there is absolutely nothing in Linnakangas about the local hosts 5 (first computer) negotiating a security association with the remote hosts 4 (second computer) so that a security association extends all the way from one of the local hosts 5 to one of the remote hosts 4. Appellants assert that Linnakangas and the other cited references completely fail to teach or suggest the step of the local hosts 5 (first computer)

establishing secure connections with the remote hosts 4 (second computer). On the contrary, Linnakangas' local hosts 5 and the router 2 communicate, as indicated above, via a Local Area Network (LAN) 1. The SA thus only extends between the remote hosts 4 and the router 2 but not between the router 2 and the local hosts 5. To further support that there is no security association established between the router 2 and the local hosts 5, the router 2 decrypts, reads and unwraps any secure message received from the remote hosts 4 to be able to determine that the message is to be forwarded (most likely as plain text) to the local hosts 5. This forwarding is done without implementing IPSec. There is nothing about forming a secure message in the local hosts 5 or the local hosts 5 negotiating secure associations with the remote hosts 4. In other words, it is important to note that the negotiated secure connection merely extends between the router 2 and the remote hosts 4. On page 4 of the Office action, the Examiner refers to paragraph 8, lines 1-5 of Linnakangas as teaching that "the destination of the packets is the second computer." Firstly, the claim does not require that the "destination of the packets is the second computer." The claim requires that the secure connection has a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection. As explained above, Linnakangas' SA

only extends between the intermediate computer (router 2) and the remote hosts (4) but excludes the segment between the router (2) and the local hosts (5). Secondly, the cited text segment in paragraph 8, lines 1-5 of Linnakangas merely refers to the IP forwarder as being the receiver (or "destination" as the Examiner calls it). It is important to realize that the IP forwarder is an inner destination within the router 2 itself and not the local hosts (5). Paragraph 31, lines 1-3 of Linnakangas supports this. The IP forwarder (IPFW) is shown in Fig. 2 that describes the internal architecture of the router 2 (see paragraph 21 of Linnakangas). In paragraph 24, lines 4-8, Linnakangas explains that "[b]y using IPSec to control communication between the router 2 and the remote hosts 4 (and hence between remote hosts 4 and local hosts 5), a Virtual Private Network (VPN) may be established" (emphasis added). It is respectfully submitted that this is different from establishing a secure connection that extends all the way from the local hosts 5 to the remote hosts 4 which requires the exchange of keys according to a key exchange protocol. Additionally, "controlling" communication across the route from local hosts 5 via router 2 all the way to the remote hosts 4 does not mean that there is a secure connection established also between router 2 and host 5. As explained above, the nodes involved in the negotiation and exchange of keys according to the key exchange protocol IKE determines the

boundaries of the secure connection. In Linnakangas, the exchange of keys is only between the router 2 and the remote hosts 4. In other words, Linnakangas merely mentions controlling the communication, not securing. It should be noted that the virtual private network in Linnakangas is not secured since it is not part of the security association between the router 2 and the remote hosts 4. There is not really as much need for a secure connection between the router 2 and the host 5 since the connection is within the same LAN.

Even if the communication between the router 2 and the local hosts 5 may be considered quite safe, it is still not part of the SA because the SA merely extends between the router 2 and the remote hosts 4. The fact that there is no SA between the router 2 and the local hosts 5 is supported on line 2 of paragraph 4 in Linnakangas that discusses encapsulation and decapsulation of IPSec packets. This means the segment between the router 2 and the local hosts 5 is not part of the security association that extends between the router 2 and the remote hosts 4. If this segment would have been part of the same security association then there would not make sense to encrypt and decrypt incoming and outgoing messages between the router 2 and the local hosts 5. Instead, the packets are opened and decrypted by adding an IPSec layer. This is quite different from address substitution in a secure connection that extends between

the first computer and the second computer as required by claim 1. In other words, when the router 2 receives a packet from the outside (such as from the remote hosts 4), the router 2 opens the packet (decapsulation) and sends it to the local host 5 in a decrypted form and when the router 2 receives a packet from within the network (such as from the local hosts 5) the router encrypts the packets by adding an IPSec layer and sends it into the security association (SA) such as to the remote hosts 4.

On page 5 of the Office action, the Examiner states that the router is able to perform IPSec and IKE translation and inherently includes a translation table. Appellants cannot see that Linnakangas teaches that the router 2 can perform IPSec/IKE translation as asserted by the Examiner. The Examiner also states that "address substitution is a standard part of IPSec processing and IKE translation." It should be noted that address substitution is not a standard part of IPSec. The Examiner refers to paragraphs 4 and 24 of Linnakangas as teaching that address substitution is standard.

In view of the above, it is submitted that claim 1 is not anticipated by Linnakangas and that the Section 102 rejection should be withdrawn.

Claims 2-5 and 7-10 are submitted to be allowable because they depend upon the allowable base claim 1 and because each claim includes limitations that are not taught or suggested

in the cited references.

Claim 22 is submitted to be allowable for reasons similar to the arguments put forth for the allowability of claim 1. As mentioned above, Linnakangas merely shows the establishment of a secure connection between the remote hosts 4 and the router 2 by negotiating security associations (SAs) between those two components. Appellants fail to see where Linnakangas teaches means for negotiating and exchanging keys, according to a key exchange protocol, between the local hosts 4 (first computer) and the remote hosts 5 (second computer) to establish a security association that has a source address of the local host 5 as a first end point and a destination address of the remote host 4 as a second end point, as required by claim 22. In contrast, Linnakangas merely teaches the negotiation of the security associations between the router 2 (intermediate computer) and the remote hosts 4 (second computer), as expressly shown in paragraph 0024 of the Linnakangas reference and as explained above.

It is submitted that Linnakangas fails to teach or suggest all the limitations of claim 22. Therefore, the anticipation rejection of claim 22 under § 102 is improper, and should be removed.

Claims 23-24 and 26 are submitted to be allowable because the claims depend either directly or indirectly upon the

allowable base claim 22 and because each claim includes limitations that are not taught or suggested in the cited references.

Similar to claim 22, claim 27 requires means for negotiating and exchanging keys between the first computer and the second computer to establish a secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point. For reasons similar to the reasons put forth for the allowability of claims 1 and 22, claim 27 is submitted to be allowable.

Argument (Rejection 2, Claims 6, 11-14, 20-21) - 35 U.S.C. 103 (Obviousness)

Claims 6, 11-14 and 20-21 are submitted to be allowable because the claims depend upon the allowable base claim 1 and because the claims include limitations that are not taught or suggested in the cited references.

Additionally, the latest Section 103 obviousness rejection is submitted to be improper because the Examiner has applied the incorrect standard. On page 3 of the Office action of 23 March 2010 the Examiner writes "[t]he rationale for the combination of the references comes from a motivation that is obvious to one of ordinary skill in the art, and does not have to come from the cited references themselves. In this case, the

examiner feels that the increased security on a network is a motivation to combine one reference with another."(emphasis added). This is clearly not the obviousness standard as set out by the courts. The Examiner seems to use his own subjective standard for what he "feels" is a good rationale for the combination without finding support for the asserted rationale in the cited references. Appellants submit that this subjective or personal standard of the Examiner is not what the courts have ruled to be the proper standard.

Even assuming *arguendo* that the requisite method steps of claims 6, 11-14 and 20-21 are shown by the combination of Linnakangas and AAPA, *prima facie* support for combining the references, according to the requirements as set forth in M.P.E.P. § 2142 has not been provided in the Office Actions.

As provided in M.P.E.P. § 2142, the Supreme Court in *KSR International v. Teleflex Inc.*, 82 USPQ2d 1385, 1396 (2007) specified that the analysis supporting a rejection under 35 U.S.C. § 103 should be made explicit. "[R]ejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3dd 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006). Furthermore, the Examiner must make "explicit" this rationale of "the apparent reason to combine the

known elements in the fashion claimed," including a detailed explanation of "the effects of demands known to the design community or present in the marketplace" and "the background knowledge possessed by a person having ordinary skill in the art" (KSR, page 14).

The only rationale provided in support of the 103(a) rejection of claim 6 is at the bottom of page 7 of the Office action, which merely asserts it would have been obvious to modify the teaching method of Linnakangas with AAPA because it "would have added flexibility by allowing different networks to connect to the system"(emphasis added). The Examiner has merely provided one benefit, or advantage of the modification as the only rationale provided in the Office Action in support of the instant rejection.

However, merely stating that a benefit of the modification exists, as done above, does not provide the "articulated reasoning with some rationale underpinning to support the legal conclusion of obviousness, required under *KSR*. By definition, every patentable invention must be "beneficial" - and *arguendo* every invention contemplates at least some new benefit(s) in arriving at the invention - certainly this does not render the benefit obvious or expected. Because every modification or element has a corresponding use or benefit, the above reasoning could be applied to any improvement. It appears

therefore that "hindsight construction" may have perhaps played a role in arriving at the present ground for rejection in the Office action - which though difficult perhaps to avoid in many cases, is nonetheless impermissible in making a *prima facie* showing of obviousness.

According to M.P.E.P. 2142, "the examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness" (emphasis added). It is respectfully submitted that the Examiner has not factually supported the prima facie conclusion of obviousness. Appellants cannot see that any of the cited references discusses that "one of the most important factors that has shaped the computer and networking industry is compatibility" or that allowing for "different computers, or different networks, to communicate with each other is always at the forefront of designer's mind." Additionally, Appellants cannot find that the cited references mention that since "very sensitive information can be passed over an un-trusted network such as the Internet, engineers are always looking for ways to beef-up security, and make it harder for hackers to intercept their Internet traffic." It is respectfully submitted that the above text segments are merely speculations on behalf of the Examiner and that the rationale provided by the Examiner is not

supported in the cited references. Because a *prima facie* conclusion of obviousness has not been provided in the Office Action, Appellants respectfully request reconsideration and withdrawal of this ground for rejection.

Appellants further submit that it would not be obvious to modify Linnakangas to meet all the limitations of claim 1. It is submitted Linnakangas does not provide one of ordinary skill in the art the motivation to make the required modifications needed to arrive at the claimed invention. In In re Fine, 5 USPQ2d (Fed. Cir. 1988), the court ruled (on page 1944) that there must be a motivation for the required modification to be obvious. In Winner International Royalty Corp. v. Wing, 48 USPQ2d 1139, the court ruled (on page 1144) that there must have been some explicit teaching or suggestion in the art to motivate one of ordinary skill in the art to make the required modifications.

It is submitted that Linnakangas fails to provide such explicit teaching. Additionally, there is no desirability or motivation to make the required modifications because the current system is complete and functional since the router is a firewall to the Internet 3 for the local area network (LAN) 1. The IP forwarder in the router 2 is designed to open incoming packets (decapsulation) and sends them to the local hosts 5 in a decrypted form and when the router 2 receives outgoing packets

from within the network (i.e. from the local hosts 5) the router encrypts the packets by adding an IPSec layer and sends them to the outside receives such as to the remote hosts 4. This function of the IP forwarder would be useless if the security associations were to be extended all the way to the local hosts 5. The extension of the security association all the way to the local hosts 5 would even make Linnakangas' system inoperable because the decapsulation would interfere with the protocol of the security association. Even if one could find reasons to make the required modifications of Linnakangas' system, Linnakangas and the other cited references still completely fail to teach or suggest the required modifications.

It is thus submitted it would not be obvious to modify Linnakangas to substitute addresses in the same security association and to extend the security association to the local hosts 5 because Linnakangas does not teach or suggest these modifications and it would, among other things, interfere with the function of the IP forwarder.

In view of the above, it is submitted that the claims 6, 11-14 and 20-21 are allowable.

Argument (Rejection 3, Claims 15-19 and 25) - 35 U.S.C. 103 (Obviousness)

Claims 15-19 and 25 are submitted to be allowable because the claims depend upon the allowable base claim 1 and 25, respectively, and because the claims include limitations that are not taught or suggested in the cited references. In this rejection, the Examiner has provided additional "benefits" without providing any rationale for why the combination is obvious. The Examiner merely states (page 11, lines 11-12 of the Office action) that the combination of Linnakangas with Sandhu would have "added another layer of security within the secure connection." On page 12, lines 5-6, the Examiner states that the proposed combination would "have increased the number of security features available in the system." It is submitted that the rationale provided by the Examiner does not satisfy the requirement of providing some articulated reasoning with some rational underpinning, as explained above.

In view of the above, it is submitted that the claims 15-19 and 25 are allowable.

In view of the above arguments, Appellants respectfully request that the Board reverse the Examiner's rejections.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/
Rolf Fasth
Registration No. 36,999

FASTH LAW OFFICES
26 Pinecrest Plaza, Suite 2
Southern Pines, NC 28387-4301
Telephone: (910) 687-0001
Facsimile: (910) 295-2152

Claims Appendix

1. (Previously presented) A method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network, comprising:
the first computer and the second computer negotiating and exchanging keys according to a key exchange protocol to establish a secure connection between the first computer and the second computer via the intermediate computer, the secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection,
in the first computer, forming a secure message by giving the secure message a first unique identity and a first destination address to the intermediate computer,
sending the secure message from the first computer to the intermediate computer,
the intermediate computer receiving the secure message and performing a translation by using the first unique identity to find a second destination address to the second computer,
the intermediate computer substituting the first destination address with the second destination address to the second computer,
the intermediate computer substituting the first unique identity with a second unique identity of the secure connection without

establishing a new secure connection and without involving the second computer, and

the intermediate computer forwarding the secure message with the second destination address and the second unique identity to the second computer in the secure connection.

2. (Previously presented) The method of claim 1 wherein the method further comprises forming the secure message by using an IPSec connection between the first computer and the second computer.

3. (Previously presented) The method of claim 1 wherein the method further comprises performing a secure forwarding of the message by making use of SSL or TLS protocols.

4. (Previously presented) The method of claim 2 wherein the method further comprises manually performing a preceding distribution of keys to components for forming the IPSec connection.

5. (Previously presented) The method of claim 2 wherein the method further comprises performing a preceding distribution of keys for forming the IPSec connection by an automated key exchange protocol.

6. (Previously presented) The method of claim 5 wherein the method further comprises performing the automated key exchange protocol used for the preceding distribution of keys for forming the IP Sec connection by means of a modified IKE key exchange protocol between the first computer and the intermediate computer and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer.

7. (Previously presented) The method of claim 2 wherein the method further comprises sending the message that is sent from the first computer as a packet that contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer, the unique identity.

8. (Previously presented) The method of claim 1 wherein the method further comprises the IPSec connection being one or more security associations (SA) and the unique identity being one or more SPI values.

9. (Previously presented) The method of claim 1 wherein the method further comprises performing the matching by using a

translation table stored at the intermediate computer.

10. (Previously presented) The method of claim 1 wherein the method further comprises changing both the address and the SPI-value by the intermediate computer.

11. (Previously presented) The method of claim 1 wherein the method further comprises the first computer being a mobile terminal so that the mobility is enabled by modifying the translation table at the intermediate computer.

12. (Previously presented) The method of claim 11 wherein the method further comprises performing the modification of the translation tables by sending a request for registration of the new address from the first computer to the intermediate computer.

13. (Previously presented) The method of claim 12 wherein the method further comprises sending a reply to the request for registration from the intermediate computer to the first computer.

14. (Previously presented) The method of claim 12 wherein the method further comprises authenticating or encrypting by IPSec the request for registration and/or reply.

15. (Previously presented) The method of claim 4 wherein the method further comprises establishing the key distribution for the secure connections by establishing an IKE protocol translation table, and using the translation table to modify IP addresses and cookie values of IKE packets in the intermediate computer.

16. (Previously presented) The method of claim 15 wherein the method further comprises establishing the key exchange distribution by:
generating an initiator cookie and sending a zero responder cookie to the second computer,
generating a responder cookie in the second computer,
establishing a mapping between IP addresses and IKE cookie values in the intermediate computer, and
using the translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets.

17. (Previously presented) The method of claim 15 wherein the method further comprises modifying a modified IKE protocol between the first computer and the intermediate computer by transmitting the IKE keys from the first computer to the

intermediate computer in order to decrypt and modify IKE packets.

18. (Previously presented) The method of claim 15 wherein the method further comprises carrying out in a modified IKE protocol between the first computer and the intermediate computer the modification of the IKE packets by the first computer with the intermediate computer requesting such modifications.

19. (Previously presented) The method of claim 17 wherein the method further comprises defining the address so that the first computer is identified for the second computer by the intermediate computer by means of an IP address taken from a pool of user IP addresses when forming the translation table.

20. (Previously presented) The method of claim 1 wherein the method further comprises sending the secure message by using an IPSec transport mode.

21. (Previously presented) The method of claim 1 wherein the method further comprises sending the secure message by using an IPSec tunnel mode.

22. (Previously presented) A telecommunication network for secure forwarding of messages, comprising:

a first computer, a second computer and an intermediate computer,

means for negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a security association having a source address of the first computer as a first end point and a destination address of the second computer as a second end point,

the first and the second computers having means for performing an IPSec processing,

the intermediate computer having translation means for using translation tables to perform IPSec and IKE translation and for changing a destination address of the intermediate computer of a secure message to a destination address of the second computer, and

the intermediate computer having means for forwarding the secure message received from the first computer to the second computer in the security association.

23. (Previously presented) The telecommunication network of claim 22 wherein the translation table for IPSec translation has IP addresses of the intermediate computer to be matched with IP addresses of the second computer.

24. (Previously presented) The telecommunication network of claim

22 wherein the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate computer and the second computer.

25. (Previously presented) The telecommunication network of claim 24 wherein both partitions of the mapping table for IKE translation contains translation fields for a source IP address, a destination IP address, initiator and responder cookies between respective computers.

26. (Previously presented) The telecommunication network of claim 22 wherein there is another translation table for IKE translation containing fields for matching a given user to a given computer.

27. (Previously presented) A telecommunication network for secure forwarding of messages, comprising:
a first computer,
a second computer,
an intermediate computer electronically connected to the first computer and the second computer,
means for negotiating and exchanging keys between the first computer and the second computer to establish a secure connection

having a source address of the first computer as a first end point and a destination address of the second computer as a second end point, and

the intermediate computer having means for performing translation between destination addresses and secure identities for forwarding secure messages received from the first computer to the second computer in the secure connection.

Evidence Appendix

There is no evidence to be presented in this appendix.

Related Proceedings Appendix

There is no related proceeding to be presented in this appendix.